UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/833,173	04/11/2001	Jeffrey Jonathan Spurgat	10587.0056-00000	1523

22852 7590 01/22/2010

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
CHOUDHURY, AZIZUL Q	
ART UNIT	PAPER NUMBER
2445	

MAIL DATE	DELIVERY MODE
01/22/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/833,173	SPURGAT ET AL.	
	Examiner	Art Unit	
	AZIZUL CHOUDHURY	2445	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 September 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____ .

Detailed Action

This office action is in response to the correspondence received on September 30, 2009.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones et al (US Pat No: 6,697,944) in view of Wiser et al (US Pat No: 6, 868,403), hereafter referred to as Jones and Wiser, respectively.

1. With regards to claim 1, Jones teaches through Wiser a secure architecture for preventing copying of digital content by way of a computing platform, the secure architecture comprising: a secure computing platform for receiving and storing encrypted digital content from the Internet and from a remote source of digital content (*Jones teaches a trusted PC connecting to the Internet/digital content provider server (remote source); see column 8, lines 19-25 and lines 40-67, Jones*) as well as storing local encrypted data, and processing said encrypted digital data (*Jones teaches the downloading (storing) of encrypted music and*

allowing for playback of the encrypted music by decrypting; see column 8, lines 62-65, Jones), said computing platform including a host processor and a peripheral bus *(equivalent to USB in Jones' disclosure; see column 9, lines 41-52, Jones)*, said computing platform configured to maintain said digital content in encrypted form so as to eliminate unauthorized distribution and run audio or video playback application software for passing said encrypted digital data to said peripheral bus *(Jones teaches the PC having playback means for encrypted music; see column 9, lines 15-20 and column 10, lines 9-18, Jones)*, a playback device including a separate content processor and a peripheral bus interface for receiving said encrypted digital content from said peripheral bus said content processor configured to decrypt said encrypted digital content and control playback of said digital content by said playback device, said playback device also including a memory device for storing decryption software *(Jones teaches the portable device (playback device) having receiving encrypted music via USB (peripheral bus interface); see column 10, lines 9-18 and 28-32, Jones. Jones also teaches the playback device having decryption means or even having means to download decryption software (both equivalent to storing decryption software); see column 12, lines 30-47, Jones. The playback device is an mp3 player and it is implicit that an mp3 player has a content processor since it processes content; see column 12, lines 48-66, Jones)*, said playback device configured to decrypt said encrypted digital data and generate a decrypted output signal for playback *(Jones teaches the portable device decrypting the encrypted*

music; see column 12, lines 30-47, Jones), said playback device configured so that computing platform can not access said decrypted digital content from said playback device when said playback device is connected to said computing platform, wherein said computing platform and said playback device are configured to download encrypted digital content from said computing platform to said playback device whenever playback device issues a download command to said computing platform *(Jones teaches the portable device (playback device) controlling the download (download command) after being connected to a computing platform. Encrypted files are sent to the portable device when the portable device has decryption means; see column 11, lines 45-61 and column 12, lines 30-47, Jones).*

While Jones' design teaches the use of digital content for providing music, Jones does not explicitly cite the computing platform being restricted from accessing decrypted digital content when the playback device is connected to it.

In the same field of endeavor, Wiser teaches a media player that connects to a host (column 3, lines 39-52, Wiser). The design features a media player (equivalent to the claimed playback device) with decryption means for purchased music. Wiser teaches how the purchased music can only be decrypted and played back on the specific media player and no other device (column 3, lines 39-52, Wiser). By having digital content only readable by a specific device, the seller of the digital content ensures copyright protections are not violated. It therefore would have been obvious to one skilled in the art, during the time of the

invention, to have combined the teachings of Jones with those of Wiser to secure online music to avoid copyright infringements (see column 3, lines 2-11, Wiser).

2. With regards to claim 2, Jones teaches through Wiser the secure architecture, wherein said computing platform includes a network interface for receiving digital data from an external network (column 7, lines 38-40, Jones).

3. With regards to claim 3, Jones teaches through Wiser the secure architecture, wherein said peripheral bus is a USB bus (column 9, lines 37-53, Jones).

4. With regards to claim 4, Jones teaches through Wiser the secure architecture, wherein said peripheral bus is a PCI bus (column 9, lines 37-53, Jones).

5. With regards to claim 5, Jones teaches through Wiser the secure architecture, wherein said peripheral bus is a Fire Wire bus (Jones' design allows for the use of buses, it would have been obvious to have used a FireWire bus; column 9, lines 37-53, Jones).

6. With regards to claim 6, Jones teaches through Wiser the secure architecture further including one or more user input devices (Figure 1, elements 40 and 42, Jones).

7. With regards to claim 7, Jones teaches through Wiser the secure architecture, wherein said computing architecture includes one or more local persistent storage devices (Figure 1, elements 29 and 60, Jones).

8. With regards to claim 8, Jones teaches through Wiser a secure hardware architecture for preventing copying of digital content by way of a computing platform, the secure architecture comprising: a computing platform for receiving and storing encrypted or encoded digital content from the Internet as well as storing local encrypted or encoded data (*Jones teaches a trusted PC connecting to the Internet/digital content provider server; see column 8, lines 19-25 and lines 40-67, Jones*), and processing said encrypted or encoded digital data, said computing platform including a host processor and a peripheral bus, said computing platform configured to run audio or video playback application software for passing said encrypted or encoded digital data to said peripheral bus, said computing platform configured so that said peripheral bus is not accessible by said audio or video playback software running on said computing platform (*Jones teaches the downloading (storing) of encrypted music and allowing for playback of the encrypted music by decrypting; see column 8, lines 62-65, Jones. Jones also teaches USB (peripheral bus); see column 9, lines 41-52, Jones*); a playback device configured to be connected to said computing platform for receiving encrypted or encoded digital content from said computing platform, said playback device including a separate processor, a peripheral bus

interface for receiving said encrypted or encoded digital signals from said peripheral bus and decrypting or decoding said encrypted or encoded data signals, said playback device also including a memory device for storing decoding or decryption software, said peripheral interface coupled to said peripheral bus for receiving said encrypted and encoded digital signals from said peripheral bus, said playback device configured to decrypt or decode said encrypted or encoded digital data and generate a decoded or decrypted analog output signal for playback *(Jones teaches the portable device (playback device) having receiving encrypted music via USB (peripheral bus interface); see column 10, lines 9-18 and 28-32, Jones. Jones also teaches the playback device having decryption means or even having means to download decryption software (both equivalent to storing decryption software); see column 12, lines 30-47, Jones. The playback device is an mp3 player and it is implicit that an mp3 player has a content processor since it processes content; see column 12, lines 48-66, Jones)*, wherein said playback device is configured to create a list of decrypted or decoded digital content stored on said playback device *(Jones' disclosure teaches the listing of decrypted files; see column 12, line 65 - column 13, line 1, Jones)*, wherein said computing platform and said playback device are configured to download encrypted digital content from said computing platform to said playback device whenever said playback device issues a download command to said computing platform *(Jones teaches the portable device (playback device) controlling the download (download command) after being*

connected to a computing platform. Encrypted files are sent to the portable device when the portable device has decryption means; see column 11, lines 45-61 and column 12, lines 30-47, Jones).

While Jones' design teaches the use of digital content for providing music, Jones does not explicitly cite the computing platform being restricted from accessing decrypted digital content when the playback device is connected to it.

In the same field of endeavor, Wiser teaches a media player that connects to a host (column 3, lines 39-52, Wiser). The design features a media player (equivalent to the claimed playback device) with decryption means for purchased music. Wiser teaches how the purchased music can only be decrypted and played back on the specific media player and no other device (column 3, lines 39-52, Wiser). By having digital content only readable by a specific device, the seller of the digital content ensures copyright protections are not violated. It therefore would have been obvious to one skilled in the art, during the time of the invention, to have combined the teachings of Jones with those of Wiser to secure online music to avoid copyright infringements (see column 3, lines 2-11, Wiser).

9. With regards to claim 9, Jones teaches through Wiser, the secure architecture, wherein said playback device is further configured to enable editing of said list *(Wiser teaches the organizing of play lists (equivalent to the claimed editing of list); see column 10, lines 7-13, Wiser).*

10. The obviousness motivation applied to claims 1 and 8 are applicable to their respective dependent claims.

Response to Remarks

The amendment received on September 30, 2009 has been carefully examined but is not deemed fully persuasive. However, the amended claims do not overcome the previously issued 103. The following are the examiner's response to the applicant's argument.

The principle argument presented by the applicant concerns the claimed secure architecture for protecting downloaded digital content even when the relationship between the computing platform and the playback device is not a trusted relationship. The applicant contends that neither prior art teaches this feature. The examiner respectfully disagrees.

First, it is noted that the exact features upon which applicant relies (i.e., *trust relationships*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The claims only state that decrypted digital content is inaccessible by said computing platform when it is connected to the playback device.

Furthermore, Wiser teaches how the purchased music can only be decrypted and played back on the specific media player (playback device) and no other device (column 3, lines 39-52, Wiser) (hence protection from unauthorized redistribution of

decrypted content). Finally, Jones also teaches how encrypted files are transferred from a computing device to a portable device (playback device) wherein the decryption occurs at the portable device (to prevent unauthorized access of the digital content (column 11, lines 45-61 and column 12, lines 30-47, Jones).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AZIZUL CHOUDHURY whose telephone number is (571)272-3909. The examiner can normally be reached on M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Vivek Srivastava can be reached on (571) 272-7304. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/A. C./
Examiner, Art Unit 2445

/Rupal D. Dharia/
Supervisory Patent Examiner, Art Unit 2400